Dana Cimera, Esq.
FITAPELLI & SCHAFFER, LLP
28 Liberty Street
New York, New York 10005
Telephone: (212) 300-0375
E-mail: DCimera@FSLawFirm.com

David C. Silver, Esq. (*pro hac vice forthcoming*)
SILVER MILLER
4450 NW 126th Avenue - Suite 101
Coral Springs, Florida 33065
Telephone: (954) 516-6000
E-Mail: DSilver@SilverMillerLaw.com

Attorneys for Plaintiff William Rose

UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY

----------X

WILLIAM ROSE, an individual,

Plaintiff,

v.

CELLULAR TOUCH WIRELESS, INC., a Florida corporation;

Defendant.

----------X

Miscellaneous Action No. _____

Motion Day: January 16, 2024

PLAINTIFF'S MEMORANDUM OF LAW IN SUPPORT OF MOTION TO COMPEL COMPLIANCE WITH NON-PARTY SUBPOENAS SERVED UPON T-MOBILE USA, INC.

Plaintiff WILLIAM ROSE, an individual ("Plaintiff"), by and through his undersigned counsel and pursuant to Federal Rules of Civil Procedure 7(b) and 45 and Local Civil Rule 7.1, hereby submits this memorandum of law in support of his motion requesting that this Honorable Court enter an Order compelling compliance with non-party subpoenas served upon T-Mobile USA, Inc. and entering all appropriate relief in connection therewith, as set forth herein.

In support of his motion, Plaintiff states:

FACTUAL BACKGROUND AND PROCEDURAL HISTORY

THE LAWSUIT

1. On January 11, 2023, Plaintiff filed his Complaint for Damages and Equitable Relief in the matter styled William Rose v. Cellular Touch Wireless, Inc., United States District Court - Southern District of Florida - Case No. 2:23-cv-00022-JLB-KCD (the "Lawsuit") [SD Fla. DE 1], a true and correct copy of which is attached as **Exhibit "A"** to the Declaration of David C. Silver, Esq. ("Silver Decl.") filed simultaneously herewith.

2. The Lawsuit is brought by Plaintiff, a Metro by T-Mobile subscriber who lost approximately Two Hundred Eighty Thousand Dollars ($280,000.00) worth of cryptocurrency in August 2021 in an under-recognized identity theft crime called "SIM swapping" or "SIM hijacking."

3. Defendant CELLULAR TOUCH WIRELESS, INC. ("Defendant") is an Exclusive Indirect Dealer who operates retail store locations in Florida under the brand of cellular telecommunications provider Metro by T-Mobile -- a discount service provider in the T-Mobile USA, Inc. ("T-MOBILE") family of companies and the telecom provider through whom Plaintiff received his monthly cellphone service.

4. According to an August 27, 2021 press release issued by T-Mobile and its Chief Executive Officer Mike Sievert, "*On August 17th, we confirmed that T-Mobile's systems were subject to a criminal cyberattack that compromised data of millions of our customers, former customers, and prospective customers.*" *See*, Silver Decl. at **Exhibit "B"**.

5. The August 2021 T-Mobile press release went on to state:

> ***Today I'm announcing that we have entered into long-term partnerships with the industry-leading cybersecurity experts at Mandiant, and with consulting firm KPMG LLP. We know we need additional expertise to take our cybersecurity efforts to the next level -- and we've brought in the help.*** *These arrangements are part of a substantial multi-year investment to adopt best-in-class practices and transform our approach. This is all about assembling the firepower we need to improve our ability to fight back against criminals and building a future-forward strategy to protect T-Mobile and our customers.*

> ***As I previously mentioned, Mandiant has been part of our forensic investigation since the start of the incident, and we are now expanding our relationship to draw on the expertise they've gained from the front lines of large-scale data breaches and use their scalable security solutions to become more resilient to future cyber threats. They will support us as we develop an immediate and longer-term strategic plan to mitigate and stabilize cybersecurity risks across our enterprise.***
>
> *Simultaneously, we are partnering with consulting firm KPMG, a recognized global leader in cybersecurity consulting. KPMG's cybersecurity team will bring its deep expertise* ***and*** *interdisciplinary approach to perform a thorough review of all T-Mobile security policies and performance measurement. They will focus on controls to identify gaps and areas of improvement.* ***Mandiant and KPMG will work side-by-side with our teams to map out definitive actions that will be designed to protect our customers and others from malicious activity now and into the future. I am confident in these partnerships and optimistic about the opportunity they present to help us come out of this terrible event in a much stronger place with improved security measures.***

(emphasis added).

6. Documents maintained by, *inter alia*, Defendant, T-MOBILE, Metro by T-Mobile, Mandiant, and KPMG demonstrate that employees or employee credentials at a Defendant store location were used to effectuate the unauthorized SIM swap and account takeover imposed upon Plaintiff, which was vital in the scheme to steal Plaintiff's assets – a scheme that exploited certain internal cybersecurity flaws known to Metro by T-Mobile, T-MOBILE, Defendant, Mandiant, and KPMG yet not adequately remedied and which exposed Plaintiff to the harm he suffered.

7. For example, when engaging Mandiant and KPMG in 2021 to thoroughly review all of T-MOBILE'S security policies and performance measurements to identify gaps and areas of improvement, T-MOBILE gave Mandiant and KPMG consultants e-mail addresses using the "@t-mobile.com" domain and gave them accounts providing access to T-MOBILE'S Microsoft SharePoint platform to communicate with T-MOBILE about the problems identified -- a decision designed to hide that information and frustrate discovery of those communications related to the T-MOBILE security breaches and Mandiant and KPMG's proposed solutions thereto.

8. As a result of those reviews and communications between MANDIANT and T-Mobile, recommendations were presented to T-Mobile: (a) addressing some of the problems that persisted at the time Plaintiff's account was hacked, and (b) offering scalable security solutions for T-Mobile to become more resilient to future cyber threats – subjects that are unquestionably relevant to Plaintiff's claim in this matter and the cybersecurity flaws that led, in large part, to the harm addressed in his Complaint.

9. Plaintiff's Complaint makes the relevance of that information plainly clear. The following are but a few examples from the Complaint of why it is relevant:

> PARAGRAPH 28: SIM swaps are commonly executed by attackers who gain authorized or unauthorized access to a wireless provider's computer networks or who gain such access with the assistance of witting or unwitting individuals who had access to the telecommunications provider's networks.
>
> * * *
>
> PARAGRAPH 52: Upon further information and belief, Defendant was aware that its security systems and internal software platform contained significant holes and weaknesses that permitted unchecked security bypasses and allowed unauthorized actors to enter the system and gain control over customer accounts and information; yet Defendant did not take adequate measures to address those holes and weaknesses.
>
> * * *
>
> PARAGRAPH 92: Defendant likewise knew that Plaintiff's Personal Information was vulnerable to hacks by thieves and other criminals because, inter alia, Metro by T-Mobile acknowledged such in its Privacy Policy, COBC, and CPNI Policy.
>
> PARAGRAPH 93: Defendant thus knew of the substantial and foreseeable harms that could occur to Plaintiff if Defendant did not place adequate security on Plaintiff's Personal Information and did not follow its own security measures for Plaintiff's account.
>
> * * *
>
> PARAGRAPH 95: Plaintiff signed up for Metro by T-Mobile's wireless services and agreed to provide his Personal Information to Metro by T-Mobile with the understanding that Metro by T-Mobile and its agents would take appropriate measures to protect it. But Defendant -- acting as an authorized agent of Metro by T-Mobile -- did not protect Plaintiff's Personal Information and violated his trust.
>
> PARAGRAPH 96: Defendant knew its security was inadequate.
>
> * * *

PARAGRAPH 99: Defendant breached its duty to exercise reasonable care in safeguarding and protecting Plaintiff's Personal Information, including CPI and CPNI, by failing to adopt, implement, and maintain adequate security measures to safeguard that information, including its duty under the FCA, the CPNI Rules, and its own Privacy Policy, COBC, and CPNI Policy.

PARAGRAPH 100: Defendant's failure to comply with federal and state requirements for security further evidences Defendant's negligence in failing to exercise reasonable care in safeguarding and protecting Plaintiff's Personal Information, including CPI and CPNI.

PARAGRAPH 101: But for Defendant's wrongful and negligent breach of the duties owed to Plaintiff, his Personal Information, including his CPI and CPNI, would not have been compromised, stolen, viewed, and used by unauthorized persons.

PARAGRAPH 102: Defendant's negligence was a direct and legal cause of the theft of Plaintiff's Personal Information and the legal cause of his resulting damages, including, but not limited to, the theft of approximately $280,000.00 worth of cryptocurrency.

PARAGRAPH 103: The injury and harm suffered by Plaintiff was the reasonably foreseeable result of Defendant's failure to exercise reasonable care in safeguarding and protecting Plaintiff's Personal Information, including his CPI and CPNI.

10. Plaintiff needs to obtain and rely upon the documents created and reviewed by Mandiant and KPMG to support his claims, and to overcome Defendant's anticipated defenses, in the lawsuit.

THE SUBPOENAS

The May 2023 T-Mobile Subpoena

11. On May 23, 2023, Plaintiff propounded upon non-party T-MOBILE a subpoena duces tecum in accordance with Fed.R.Civ.P. 45 (the "May 2023 T-MOBILE Subpoena"). *See*, Silver Decl. at **Exhibit "C"**.

12. The May 2023 T-MOBILE Subpoena requested that the following documents be produced by T-MOBILE in Livingston, NJ, which is approximately ten (10) miles from T-MOBILE's headquarters in Parsippany, NJ:

DOCUMENTS TO BE PRODUCED

1. All non-privileged documents in your files for Plaintiff's account at

METRO, including but not limited to the internal account notes and customer service records generated by your representatives (employees, agents, or independent contractors) relating to the unauthorized activity on Plaintiff's METRO account on or about August 13, 2021 (the "Unauthorized SIM Swap") which was detected by you/METRO and memorialized in correspondence to Plaintiff concerning a breach of Plaintiff's Customer Proprietary Network Information ("CPNI") at METRO.

2. All non-privileged documents in your files relating to the Unauthorized SIM Swap, including:

(a) all documents memorializing the identity and contact information of each person to whom Plaintiff's METRO service, SIM card, or IMEI were transferred;

(b) all documents memorializing the identity and contact information of each T-MOBILE or METRO representative (employee, agent, or independent contractor) who approved or processed the Unauthorized SIM Swap;

(c) all Amdocs IMEI Tumbling Reports that relate to or include information evidencing the Unauthorized SIM Swap;

(d) all incident reports relating to the Unauthorized SIM Swap including all investigator attachments -- however categorized or titled -- whether performed by a T-MOBILE or METRO Fraud Team, Corporate Investigation Team, Cybersecurity Team, or any other group;

(e) all Anomaly Reports -- however categorized or titled -- relating to the weekly period during which the Unauthorized SIM Swap took place;

(f) all incident reports -- however categorized or titled -- relating to the credentials flagged in any anomaly reports during the weekly period in which the Unauthorized SIM Swap took place including all Investigator Attachments -- whether performed by a T-MOBILE or METRO Fraud Team, Corporate Investigation Team, Cybersecurity Team, or any other group;

(g) All documents showing each time **SIM card number 8901260041922999537F** was used in a SIM swap or device change during the time period ranging from July 1, 2021 through September 1, 2021, including: what METRO credential was used to perform the SIM swap/device change; the name of the METRO store that corresponds to the dealer used; the date and time the SIM swap/device change was performed; and with what IMEI number the SIM card was paired with during the SIM swap/device change;

(h) All documents showing each time **IMEI number 355825089455506** was used in a SIM swap or device change during the time period ranging from July 1, 2021 through

September 1, 2021; including: what METRO credential was used to perform the SIM swap/device change; the name of the METRO store that corresponds to the dealer used; the date and time the SIM swap/device change was performed; and with what SIM card number the IMEI was paired with during the SIM swap/device change;

(i) All documents showing each time **METRO credential 42002008** was used in a SIM swap/device change during the time period ranging from July 1, 2021 through September 1, 2021; including the date and time the SIM swap/device change was performed; and with what SIM card number and IMEI were used in every SIM swap/device change made by that credential;

(j) All documents and data showing device changes made after hours or "After Hours Dealer Weekly" reports and data for the time period one month before the Unauthorized SIM swap through two weeks following the unauthorized SIM swap;

(k) All documents and data including spreadsheets for the Edge ID 42002008 dealer activity logs and EDGE ID 40018002 for the time period one month before the Unauthorized SIM swap through two weeks following the unauthorized SIM swap;

(l) any report memorializing or summarizing the root cause analysis -- however categorized or titled -- that addresses the root cause of the vulnerability that contributed to the Unauthorized SIM Swap and/or how the vulnerabilities could be addressed, whether or not the analysis refers to Plaintiff individually; and

(m) IP logs showing the intrusion into Plaintiff's METRO account as well as IP logs that show IP addresses blacklisted/negative listed as suspect because of SIM swap intrusions.

3. For the Unauthorized SIM Swap, please provide any documents or investigative records on how you or METRO identified the credentials utilized to access its platform; and if you or METRO determined that the credentials were compromised/corrupted, please provide documents that identify or memorialize how you or METRO made that determination.

4. For the Unauthorized SIM Swap, please provide any documents or investigative records you provided to law enforcement or regulatory authorities, including any documents submitted on the Data Breach Reporting Portal.

5. All contracts, agreements, or memoranda of understanding -- including, but not limited to, Exclusive Indirect Dealer Agreements -- entered into or exchanged between you and CTW.

6. All communications and documents exchanged between you and CTW relating to, referencing, or concerning the Unauthorized SIM Swap.

7. All communications and documents exchanged between you and METRO relating to, referencing, or concerning the Unauthorized SIM Swap.

8. All documents from the following T-MOBILE or METRO departments or teams relating to the unauthorized access(es) into Claimant's METRO account, the Unauthorized SIM Swap/device change of Claimant's account, the credential(s) used to access Claimant's account, and the credential(s) used to perform the Unauthorized SIM Swap on Claimant's account: (a) Law Enforcement Relations; (b) Corporate Investigations; (c) Cybersecurity; (d) Privacy; and (e) Fraud. You should include in your production all call data or detail records; any fraud forms filed; Amdocs tumbler reports; Account Takeover memos; any documents in Aurora; Escalations to Fraud Management emails; DCC or MCC reports; Splunk alerts; dealer tracker reports; correspondence; e-mails; handwritten notes; memorandums; RCA documentation; proposals; remediation plans; and any other related documents. The relevant time period for this request shall run from one month before the Unauthorized SIM Swap/device change enacted upon Claimant through the present date.

9. All non-privileged internal communications at T-MOBILE relating to, referencing, or concerning the Unauthorized SIM Swap; the METRO credential used to perform the Unauthorized SIM Swap; the SIM number used in the Unauthorized SIM Swap; the IMEI number used in the Unauthorized SIM Swap; and any METRO credentials flagged as suspicious or through an anomaly report being used during the weekly period of the Unauthorized SIM Swap. Included in this production should be all correspondence, electronic mail messages, video recordings, and messages exchanged through encrypted messaging networks (*e.g.*, Slack, Highside, Signal, WhatsApp, Telegram, and Discord), as well as any communications between the corporate investigators, field team, dealers, Privacy Department, or Fraud Department referencing or relating to the above.

13. The May 2023 T-MOBILE Subpoena was duly served upon T-MOBILE on May 25, 2023. *See*, Silver Decl. at **Exhibit "D"**.

14. On June 15, 2023, Plaintiff received from a Custodian of Records (Mr. Andrew Dios) in T-MOBILE's Legal & Emergency Response team a sworn declaration certifying that the documents enclosed therewith "*are duplicates of the original and are true and correct copies of records maintained by [T-MOBILE].*" *See*, Silver Decl. at **Exhibit "E"**. The documents produced consist of forty-three (43) Microsoft Excel Worksheets reflecting subscriber, account, and device information about different T-MOBILE subscribers (none of whom are Plaintiff). It is not apparent to Plaintiff's counsel who those subscribers are or what relevance they or the documents produced have to the lawsuit.

15. No categorized response from T-MOBILE identifying to which portion(s) of the May 2023 T-MOBILE Subpoena the company was responding was provided along with the declaration. Moreover, no explanation was provided by T-MOBILE as to why the documents produced are relevant or responsive to the May 2023 T-MOBILE Subpoena.

16. While the relevance of the documents produced by T-MOBILE remains unclear, what is very clear is that T-MOBILE's production ignored nearly all -- if not all -- of the categories of documents delineated in the May 2023 T-MOBILE Subpoena.

The September 2023 T-Mobile Subpoena

17. On September 18, 2023, Plaintiff propounded upon non-party T-MOBILE a second subpoena duces tecum in accordance with Fed.R.Civ.P. 45 (the "September 2023 T-MOBILE Subpoena"). *See*, Silver Decl. at **Exhibit "F"**.

18. The September 2023 T-MOBILE Subpoena seeks from T-MOBILE different documents than those sought by the May 2023 T-MOBILE Subpoena.

19. The September 2023 T-MOBILE Subpoena was duly served upon T-MOBILE on September 19, 2023. *See*, Silver Decl. at **Exhibit "G"**.

20. On October 3, 2023, undersigned counsel received from counsel for T-MOBILE a letter objecting to the September 2023 T-MOBILE Subpoena. Without addressing each subset of documents requested, T-MOBILE asserted the September 2023 T-MOBILE Subpoena is, as a whole, "*categorically objectionable*"; and T-MOBILE refused to provide an itemized response or any documents responsive to the September 2023 T-MOBILE Subpoena. *See*, Silver Decl. at **Exhibit "H"**.

21. Over the past five years, undersigned counsel has litigated against T-MOBILE/Metro by T-Mobile dozens if not hundreds of cases similar to the claim brought by Plaintiff in the instant matter. Undersigned counsel and counsel for T-MOBILE (Davis Wright Tremaine LLP has appeared as counsel for T-MOBILE/Metro by T-Mobile in all such cases) confer with one another by a variety

of methods (written communication, telephone, Zoom, etc.) on nearly a daily basis. Despite all of those back-and-forth communications, T-MOBILE has refused to provide Plaintiff anything other than its global objection to the September 2023 T-MOBILE Subpoena.

T-Mobile is Withholding Relevant Documents and Information

22. As noted above, T-MOBILE possesses vital information relevant to this dispute that Plaintiff cannot obtain from any other source.

23. In fact, in response to discovery demands propounded by Plaintiff upon Defendant in the Lawsuit that seek some of the same/similar documents to those sought from T-MOBILE through the May 2023 T-MOBILE Subpoena, Defendant represented that it only had a limited set of documents to provide and that the balance of documents could be obtained from T-MOBILE.

24. Moreover, in response to other non-party subpoenas served by Plaintiff in the Lawsuit that seek some of the same/similar documents to those sought from T-MOBILE through the September 2023 T-MOBILE Subpoena, Plaintiff was explicitly told to obtain those documents from T-MOBILE, who is believed to have all such documents in its possession, custody, or control. *See*, Silver Decl. at **Exhibit "I"**.

25. As of the date of this filing, T-MOBILE has thus far failed to produce any such communications in response to the subpoenas; and Plaintiff is left trapped between a rock (*e.g.*, Defendant and KPMG directing Plaintiff to T-MOBILE to obtain the relevant documents) and a hard place (T-MOBILE adamantly refusing to retreat from its entrenched global objection to Plaintiff's subpoenas).

26. On multiple occasions and in multiple forms over the past few years, different members of Davis Wright Tremaine LLP -- as counsel for T-MOBILE -- have denied that the documents sought by Plaintiff exist, *to wit*:

(a) In a February 22, 2023 letter to the arbitrator overseeing the arbitration proceeding between Plaintiff and T-MOBILE -- after the arbitrator had ruled

that any such documents that exist must be produced by T-MOBILE -- **Ellen Parodi, Esq.** represented to the arbitrator that the documents do not exist;

(b) During the February/March 2023 evidentiary hearing in that same proceeding, **David Glanton, Esq.** likewise represented to the arbitrator that the documents do not exist;

(c) On February 16, 2023, **James Moon, Esq.** represented to Plaintiff's undersigned counsel on a videorecorded Zoom meeting that the documents do not exist.

27. Notwithstanding T-MOBILE's repeated denial that the documents sought by Plaintiff exist, non-party witnesses (and fellow subpoenaed witnesses) KPMG and Mandiant have expressly stated or suggested that **the documents do exist** and that T-MOBILE is expected to have those documents in its possession, custody, or control.

28. Likewise, when T-MOBILE responded to the September 2023 T-MOBILE Subpoena, it did not simply state that the documents sought by Plaintiff do not exist. Instead, T-MOBILE asserted its global objections. Objections, however, are only posed to limit discovery when discovery is possible. If the documents truly did not exist, T-MOBILE would only have to say that the documents do not exist without feeling it necessary to pose a global objection.

29. The obstinance and gamesmanship undertaken by T-MOBILE is exemplified in recent correspondence from **Arthur Simpson, Esq.** of Davis Wright Tremaine LLP, who taunted undersigned counsel and challenged: "***Put your bar card on the line under penalty of perjury. Let's get it done.***" *See*, Silver Decl. at **Exhibit "J"**.

30. In light of the foregoing, Plaintiff requests that the Court compel T-MOBILE to provide a written response addressing each category of documents set forth in the May 2023 T-MOBILE Subpoena and the September 2023 T-MOBILE Subpoena and that T-MOBILE produce all responsive documents that exist in its possession, custody, or control without further delay.

DISCUSSION

Under Rule 45, a non-party may be compelled by subpoena to produce documents and to permit an inspection of records. *See*, Fed.R.Civ.P. 45(d), (e); and Fed.R.Civ.P. 34(c). The scope of discovery provided for under Rule 26 similarly applies to discovery sought via a Rule 45 subpoena on a non-party. *See*, Fed.R.Civ.P. 45(a)(1); *In Re Novo Nordisk Sec. Litig.*, 530 F. Supp. 3d 495, 501 (D. N.J. 2021); accord *E.S. by and through Sanchez v. Elizabeth Bd. of Educ.*, Civ. No. 20-1027, 2022 WL 2106382, at *2 (D. N.J. June 10, 2022).

A party may move to compel discovery sought through a subpoena on a non-party, and such motion "must be made in the court where the discovery is or will be taken." Fed.R.Civ.P. 37(a)(2). The movant must show that the sought after discovery from the non-party is relevant and, if it does, then "the resisting non-party must explain why discovery should not be permitted." *Biotechnology Value Fund, L.P. v. Celera Corp.*, Civ. No. 14-4046, 2014 WL 4272732, at *1 (D. N.J. Aug. 28, 2014) (citations and internal quotation marks omitted).

To determine if the sought-after documents are relevant, the Court considers, within its discretion, the specific facts at issue. *See*, *Carchietta v. Russo*, Civ. No. 11-7587, 2014 WL 1789459, at *3 (D. N.J. May 6, 2014). Whether certain documents are relevant is "viewed in light of the allegations of the complaint, not as to evidentiary admissibility." *Scouler v. Craig*, 116 F.R.D. 494, 496 (D. N.J. 1987).

Relevancy is typically viewed under Fed.R.Civ.P. 26(a)(1), which provides in pertinent part:

> Parties may obtain discovery regarding any matter, not privileged, that is relevant to the claim or defense of any party .... For good cause, the court may order discovery of any matter relevant to the subject matter involved in the action. Relevant information need not be admissible at the trial if the discovery appears reasonably calculated to lead to the discovery of admissible evidence.

Fed.R.Civ.P. 26(b)(1). Courts have construed this rule liberally, "creating a broad range for discovery which would 'encompass any matter that bears on, or that reasonably could lead to other matter that could bear on, any issue that is or may be in the case.'" *Caver v. City of Trenton*, 192 F.R.D. 154, 159

(D. N.J. 2000) (citing *Oppenheimer Fund, Inc. v. Sanders*, 437 U.S. 340, 351, 98 S.Ct. 2380, 57 LEd.2d 253 (1978); *Lesal Interiors, Inc. v. Resolution Trust Corp.*, 153 F.R.D. 552, 560 (D. N.J. 1994)). Review of all relevant evidence provides each party with a fair opportunity to "present an effective case at trial." *Id.*

In the instant case, the documents sought by Plaintiff are all relevant to the claims set forth in his Complaint; and Plaintiff proffers that he needs those documents to afford him a fair opportunity to present an effective case at trial. As demonstrated in Plaintiff's Complaint, Plaintiff intends to prove Defendant (among other things):

(a) failed to protect the confidentiality of Plaintiff's statutorily-protected personal identifying information -- including his wireless telephone number, account information, and his private communications -- and divulged that information to hackers in connection with the coordinated theft of Plaintiff's cryptocurrency assets;

(b) failed to properly implement and execute security procedures, federal CPNI Regulations, Metro by T-Mobile's/T-MOBILE's Privacy Policy and CPNI Policy, and unauthorized SIM swap protections;

(c) failed to protect its log-in and security credentials for Metro by T-Mobile's/T-MOBILE's Edge computer platform;

(d) ignored known and foreseeable threats to Metro by T-Mobile customers, including Plaintiff;

(e) overtly and intentionally ignored and bypassed numerous security protocols on Plaintiff's account -- barriers expressly represented to Plaintiff that were put in place to prevent an unauthorized SIM swap;

(f) prevented Plaintiff's authorized access to the Metro by T-Mobile services for which he paid during the critical time period in which the theft of Plaintiff's assets took place; and

(g) represented and supported a criminal syndicate aimed at stealing cryptocurrency from Metro by T-Mobile accountholders (including Plaintiff) following unauthorized SIM swaps on those Metro by T-Mobile accountholders.

As a result of the foregoing, Plaintiff will demonstrate at trial that Defendant has committed upon him numerous statutory violations (including violation of the Federal Communications Act) and tortious violations for which Defendant should be held liable. To do that, though, Plaintiff needs from T-MOBILE -- whose internal Corporate Investigations Team and Fraud Management Team,

among others, had numerous exchanges with Defendant about not just Plaintiff's individual account takeover and theft but about the widespread problems caused by Defendant that resulted in hundreds of similar customer account takeovers before Plaintiff was victimized by Defendant's malfeasance -- the documents T-MOBILE has that memorialize the depths of the wrongdoing that resulted in Plaintiff's damages.

The May 2023 T-Mobile Subpoena

In the face of this serious matter, T-MOBILE responded to the May 2023 T-MOBILE Subpoena by essentially not responding at all. Just as with a party to litigation upon whom a written discovery request is propounded, a non-party to litigation must respond to a subpoena with a specific written response to each category of documents requested.

> The same rationale for requiring that a party objecting to a request for production of documents under Fed.R.Civ.P. 34(b) must submit a written response specifying the objection to each category applies equally to the response to a subpoena duces tecum. This gives each party the opportunity to analyze the request and the corresponding objection, and gives the court a fuller record on which to base its ruling.

U.S. v. O'Neill, 619 F.2d 222, 225-226 (3d Cir. 1980). Failure to provide a written response not only waives any objections the subpoenaed non-party might have been able to raise had it timely and properly responded, it renders the non-party subject to compulsory production of all relevant documents in its possession, custody, or control. *See*, *e.g.*, *Gap Properties, LLC v. Cairo*, Case No. 19-cv-20117-KM-ESK, 2020 WL 13617139, at *1 (D. N.J. Dec. 21, 2020) (compelling production of all responsive documents from non-party who "failed to interpose general or specific objections to the Subpoenas" and made a "woefully deficient" production of "often irrelevant" documents). Moreover, in accordance with Fed.R.Civ.P. 45(g):

> Unless a non-party asserts an "adequate excuse" for failing to comply with a subpoena, or if a subpoena has not been issued in accordance with the procedure set forth in Rule 45(a)(2) and (a)(3)(b), a non-party's failure to comply with a subpoena may be deemed a contempt of court.

Arista Records, Inc. v. Flea World Inc., Civil No. 03-2670 (JBS), 2005 WL 8174784, at *2 (D. N.J. July 22, 2005).

Here, T-MOBILE -- with its billion dollar corporate treasury and deep roster of litigators across the country -- failed to provide even the most rudimentary and relevant response to Plaintiff's Subpoena. As a result, the Court should compel from T-MOBILE a written response addressing each category of documents set forth in the Subpoena and production of all responsive documents in its possession, custody, or control.

The September 2023 T-Mobile Subpoena

Just as with its response to the earlier subpoena, T-MOBILE's broad global objection to the September 2023 T-MOBILE Subpoena is likewise inadequate.

In the October 3, 2023 letter from T-MOBILE's counsel, T-MOBILE falsely asserts: "*Mr. Rose cannot articulate any cogent theory about how the August 2021 data breach played any role in the unauthorized SIM swap at issue in his case or how any cybersecurity or network security work by Mandiant and KPMG might relate to any issue in this case.*" *See*, Silver Decl. at **Exhibit "H"**. The Complaint in the Lawsuit clearly demonstrates the relevance of the cybersecurity and network security work by KPMG and Mandiant. The known weaknesses in T-MOBILE's and Defendant's security systems played a vital role in the harm that befell Plaintiff, and the documents in T-MOBILE's possession on that subject are well within the boundaries of relevance. *See, e.g.*, *Carchietta v. Russo*, Civ. No. 11-7587, 2014 WL 1789459, at *3 (D. N.J. May 6, 2014) (holding that to determine if sought-after documents are relevant, the Court considers the specific facts at issue).

Moreover, in the October 3, 2023 letter from T-MOBILE's counsel, T-MOBILE repeatedly asserts that the September 2023 T-MOBILE Subpoena imposes an "*undue burden*" upon T-MOBILE. However, T-MOBILE has not supported its claim of an "*undue burden*" with any evidence, nor did T-MOBILE seek judicial protection in the form of either a request to quash the September 2023 T-

MOBILE Subpoena or a request for a protective order. "Before a court will entertain a party's objection based on burdensome grounds, the party asserting the objections must submit an affidavit or offer evidence which reveals the nature of the burden." *Reid v. Cumberland Cty.*, 34 F.Supp.3d 396, 414 (D. N.J. 2013). T-MOBILE has clearly not satisfied its burden to support its objection, and T-MOBILE should not be permitted to withhold these relevant documents behind an arbitrary and capricious objection. *See*, *e.g.*, *Franchitti on behalf of United States v. Cognizant Tech. Sol. Corp.*, Civil Action No. 17-6317 (PGS) (RLS), 2023 WL 2759075, at *6 (D. N.J. Apr. 3, 2023) ("Having found that the sought-after documents are relevant to this matter, and without a showing of how a review or production of such documents would be burdensome in any way, the Court finds the DOJ's objection based on undue burden to be arbitrary and capricious here.").

CONCLUSION

WHEREFORE, in light of the foregoing, Plaintiff WILLIAM ROSE respectfully requests that the Court enter an Order:

(a) compelling non-party T-Mobile USA, Inc. to comply with the May 2023 T-MOBILE Subpoena by providing, within ten (10) days of the Court's Order, a request-by-request response (without objection) to each of the categories of documents sought by the May 2023 T-MOBILE Subpoena and also producing to Plaintiff all documents T-MOBILE has in its possession, custody, or control that respond to the May 2023 T-MOBILE Subpoena,

(b) compelling non-party T-Mobile USA, Inc. to comply with the September 2023 T-MOBILE Subpoena by providing, within ten (10) days of the Court's Order, a request-by-request response (without objection) to each of the categories of documents sought by the September 2023 T-MOBILE Subpoena and also producing to Plaintiff all documents T-MOBILE has in its possession, custody, or control that respond to the September 2023 T-MOBILE Subpoena

(c) awarding Plaintiff reasonable attorneys' fees and costs relative to the enforcement of the Subpoenas, and

(d) entering such other further relief as the Court deems just and proper.

Civil Rule 37.1(b) Certification

Notwithstanding standard requirements that parties to litigation meet and confer with one another in a good faith effort to resolve by agreement the issues raised by a discovery motion before seeking judicial intervention on the issue, this Court and others "have dispensed with requiring a party and non-party to meet and confer prior to filing a motion under Rule 45." *Housemaster SPV LLC v. Burke*, Civil Action No. 21-13411 (MAS), 2022 WL 17904254, at *7 (D. N.J. Dec. 23, 2022); *Clift v. City of Burlington*, No. 2:12-CV-214, 2013 WL 12347197, at *2 (D. Vt. Aug. 26, 2013) ("A non-party filing a Rule 45 motion therefore does not need to meet and confer prior with the counsel of the party serving the subpoena"); *Jackson v. AFSCME Local 196*, 246 F.R.D. 410, 413 (D. Conn. 2007) (Rule 45 does not require that the parties (and non-parties) meet and confer prior to the filing of a motion); *Travelers Indem. Co. v. Metropolitan Life Ins. Co.*, 228 F.R.D. 111 (D. Conn. 2005).

Nevertheless, Plaintiff's counsel has conferred in good faith with counsel for T-MOBILE to narrow the issues in dispute in this matter. However, those efforts have not produced any resolution of any part of this motion.

Respectfully submitted,

FITAPELLI & SCHAFFER, LLP

By: */s/ Dana Cimera*

Dana Cimera, Esq.
28 Liberty Street
New York, New York 10005
Telephone: (212) 300-0375
E-mail: DCimera@FSLawFirm.com

David C. Silver, Esq. (*pro hac vice forthcoming*)
SILVER MILLER
4450 NW 126th Avenue – Suite 101
Coral Springs, Florida 33065
Telephone: (954) 516-6000
E-Mail: DSilver@SilverMillerLaw.com

Counsel for Plaintiff William Rose

CERTIFICATE OF SERVICE

I HEREBY CERTIFY that a copy of the foregoing was electronically filed with the Clerk of Court on this 22nd day of December 2023 by using the CM/ECF system which will send a notice of electronic filing to the following CM/ECF participant(s): **All Parties and Counsel of Record**.

I FURTHER CERTIFY that a true and correct copy of the foregoing document was sent on this 22nd day of December 2023 via electronic mail to: **ARTHUR A. SIMPSON, ESQ.**, DAVIS WRIGHT TREMAINE, LLP, *Counsel for T-Mobile USA, Inc.*, 1201 3rd Avenue - Suite 2200, Seattle, WA 98101, E-mail: ArthurSimpson@dwt.com; and **JAMES MOON, ESQ.**, DAVIS WRIGHT TREMAINE, LLP, *Counsel for T-Mobile USA, Inc.*, 865 Figueroa Street - Suite 2400, Los Angeles, CA 90017, E-mail: JamesMoon@dwt.com.

/s/ Dana Cimera
DANA CIMERA